

Listing of Claims

1. (Currently amended) A user identity authentication system comprising:
an authentication client for requesting authentication of a subject;
a client interface to receive the authentication request from the authentication client;

multiple independently operated databases, each database storing information out-of-wallet data associated with the subject, the associated information out-of-wallet data being accessible only through predefined queries to identify the subject, the predefined queries defined in advance by agreement with respective owners of each of the multiple independently operated databases, and at least one of the predefined queries requiring at least one item of out-of-wallet data in an answer to the query; and

a verification engine for facilitating authentication of the subject by receiving the authentication request, selecting one or more of the predefined queries, including at least one of the predefined queries that requires at least one item of out-of-wallet data in an answer to the query, presenting the one or more selected queries to the subject via the authenticating client, receiving from the subject an answer to each of the one or more selected queries, and presenting the answer, including at least one item of out-of-wallet data, to each of the multiple independently operated databases for a validation response.
2. (Canceled)
3. (Original) The system of claim 1 further comprising a personal information database coupled to the verification engine, the personal information database containing in-wallet data identifying the subject.
4. (Previously presented) A system comprising:
an authentication client for desiring authentication of an authentication subject;
a plurality of independent database systems storing information identifying the authentication subject, the identifying information being accessible through predefined queries, the predefined queries defined in advance by agreement with the owners of each of the independent database systems; and

a verification engine to receive from the authentication subject, via the authentication client, an answer to each of the predefined queries, to obtain from each of

the plurality of independent database systems a corresponding authentication confidence for each answer, and to combine the corresponding authentication confidence for each answer into a combined authentication confidence.

5. (Currently amended) A user ~~authorization~~ identity authentication method comprising the steps of:

presenting to an authentication subject one or more predefined queries, the predefined queries defined in advance by agreement with owners of each of multiple independent databases, the multiple independent databases storing identifying information about the authentication subject;

receiving from the authentication subject an answer to each of ~~the selected~~ at least one of the predefined queries;

presenting each answer to at least one of the multiple independent databases that has corresponding identifying information;

obtaining from the multiple independent databases an authentication confidence level for each answer; and

combining the authentication confidence level for each answer into a combined confidence level for authenticating the authentication subject.

6. (Currently amended) A method of authenticating the putative identity of a subject who is an individual, the method comprising the steps of:

negotiating a predetermined set of permitted types of queries with an owner of an independent, remote, third-party database, the independent, remote, third-party database including identifying information associated with the subject;

providing a database interface for interacting with the independent, remote, third-party database without storing any significant portion of the third-party database locally, and wherein the interaction is limited to submitting a query among the predetermined set of permitted types of queries, and receiving from the third-party database a response to the permitted query;

responsive to a request from a client to authenticate the putative identity of the subject, forming a first query to elicit from the subject at least one item of information sufficient to form one of the permitted types of queries, and sending the first query to the subject via the client;

receiving identifying information associated with the subject in response to the first query to authenticate his identity, the received identifying information including at least one item of information sufficient to form one of the permitted types of queries;

forming a permitted type of query based on the received identifying information;

transmitting the formed query to the remote, third-party database; and

receiving a response from the remote, third-party database wherein the database interface does not otherwise provide access to the remote, third-party database, so that privacy of the remote, third-party database content remains under control of its owner.

7. (Cancelled).

8. (Previously presented) A method of authenticating the putative identity of a subject according to claim 6 and wherein said receiving the identifying information associated with the subject transpires in a live interaction with the subject in person.

9. (Previously presented) A method of authenticating the putative identity of a subject according to claim 6 and wherein receiving the identifying information associated with the subject is through a computer network.

10. (Previously presented) A method of authenticating the putative identity of a subject according to claim 9 including receiving the identifying information associated with the subject via the Internet.

11. (Previously presented) A method of authenticating the putative identity of a subject according to claim 6 and wherein the database interface enables interaction with multiple independent, remote, third-party databases without storing any significant portion of any of said databases locally, so that privacy of the remote, third-party database contents remain under control of their respective owners.

12. (Previously presented) A method of authenticating the putative identity of a subject according to claim 11 including receiving responses from a plurality of the remote, third-party databases and assembling the responses from the multiple databases to form a result.

13. (Previously presented) A method of authenticating the putative identity of a subject according to claim 6 and wherein the associated identifying information in the database includes out-of-wallet data associated with the subject.

14. (Previously presented) A method of authenticating the putative identity of a subject according to claim 6 including:

- presenting a predetermined question to the subject;
- receiving an answer to the question; and
- forming the database query responsive to the answer received.

15. (Previously presented) A method of authenticating the putative identity of a subject according to claim 14 including:

- forming a second question responsive to the response from the remote, third-party database;
- presenting the second question to the subject; and
- forming another database query responsive to the answer to the second question.

16. (Previously presented) The system of claim 1 wherein the authentication client includes an electronic commerce site.

17. (Previously presented) The system of claim 1 wherein the verification engine further facilitates authentication of the subject by:

- receiving the validation responses from each of the multiple independently operated databases, the validation responses including a match confidence; and
- determining an overall authentication confidence based on each of the received match confidences.

18. (Previously presented) The system of claim 4 wherein the authentication client includes an electronic commerce site.

19. (Previously presented) The system of claim 4 wherein the information identifying the authentication subject includes out-of-wallet data identifying the authentication subject.

20. (Previously presented) The method of claim 5 wherein the one or more predefined queries are presented to the authentication subject via an authenticating client.

21. (Previously presented) The method of claim 5 wherein the identifying information includes out-of-wallet data identifying the authentication subject.